Paper ID: 90226
oral

IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Space Communications and Navigation Global Technical Session (8-GTS.3)

Author: Dr. DINESH MANANDHAR
University of Tokyo, Japan

DETECTION OF GNSS SPOOF SIGNALS BY MULTIPLE PEAK ANALYSIS IN SIGNAL ACQUISITION

Abstract

Spoofing attacks on GNSS signals have become a serious issue in GNSS applications. Spoofing attacks are done to falsify the correct position data with the attacker's intended position data. Such attacks may also change velocity and time data as well. Spoofing attacks are not detectable since it is done by transmitting signals that are the same as the GNSS signals. A GNSS receiver can't differentiate between a real GNSS signal and a spoof GNSS signal. A spoof GNSS signal is designed the same way as the real GNSS signal. In order to detect spoofing attacks Galileo and QZSS have broadcasted signal authentication services that authenticate navigation messages of the signals. Galileo provides authentication services for Galileo signals. QZSS provides authentication services for QZSS (self-authentication) as well as GPS and Galileo (cross-authentication).

This paper discusses how to detect spoofing attacks by analyzing multiple peaks in the signal acquisition process. If a receiver is receiving a real signal and a spoof signal, there will be multiple peaks in the signal acquisition process. Normally, multiple peaks for the same PRN code will not be visible during the acquisition process unless there is a reflected signal with significant delays. A software-defined radio device is used to detect the multiple peaks. The digital IF signal is fed to multiple channels to process the incoming signal with different types of replica signals (different doppler frequencies). A very weak signal processing technique using coherent and non-coherent integration is also used to raise the signal gain to detect a very weak spoof signal or a very weak real signal. Once multiple peaks are detected in the acquisition process, the signals are decoded for the navigation data bits. These data bits are analyzed for signal authentication (in the case of QZSS and Galileo signals). One of the signals will pass the signal authentication test and the other peaks will fail the signal authentication since they won't be able to provide the same navigation data bits that are the same as the real signals. This method will help to detect a spoof signal that can be used to develop a Spoof-Proof GNSS receiver.